Manual de Instrução - MI

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

PARA TERCEIROS

Elaboração/Revisado por: Comitê de Segurança da Informação da BHIP

Análise e Aprovação: Alta Direção

LISTA DE TABELAS

Índice

1 Propósito

A Política de Segurança da Informação para Terceiros tem como objetivo estabelecer diretrizes para as normas e padrões de proteção da informação, abrangendo sua criação, uso, armazenamento e compartilhamento. Essa política busca garantir os pilares da segurança da informação que são a confidencialidade, disponibilidade e integridade (CID) das informações, independentemente do meio ou local em que estejam, alinhando-se à legislação vigente, às exigências de órgãos reguladores e às melhores práticas de segurança da informação.

2 Abrangência

Aplica-se a todas as partes interessadas da BHIP, incluindo, mas não se limitando a, Poder Concedente, fornecedores, parceiros comerciais, acionistas, prestadores de serviços, contratados e seus representantes, munícipes, que tenham acesso a informações corporativas e dados pessoais.

3 Referências

- Contrato AJ016/2016, seus Anexos e Aditivos publicados;
- ISO 9001 – Sistemas de Gestão da Qualidade;
- ISO 14001 – Sistemas de Gestão Ambiental;
- ISO 20000 – Tecnologia da Informação – Gestão de Serviços;
- ISO 27001 – Tecnologia da Informação – Técnicas de Segurança;
- MI-GC-18 Aviso de Privacidade Externo.

4 Termos e Definições

- Administradores: pessoas ou equipe com delegação superior para administrar um determinado ambiente informatizado;
- ANS: Acordo de Nível de Serviços - documento formal em que as duas partes definem o nível adequado do serviço a ser entregue de acordo com a necessidade do negócio;
- Aplicações Críticas: aplicações que atualizam valores, concedem autorização/vantagem ou tratam de informações sigilosas;
- Aplicativos: *softwares* de função específica adquiridos ou desenvolvidos pela BHIP;

- Ativos de T.I.: são todos os itens, físicos ou virtuais, que compõem a infraestrutura de TI de uma empresa e que geram valor para a mesma, tais como, mas não se limitando a: elementos de hardware de infraestrutura, como servidores e data centers; softwares, aplicativos e sistemas, sejam eles desenvolvidos internamente ou licenças de terceiros; dispositivos físicos como notebooks, computadores, mouses, teclados, telefones/celulares e impressoras, redes de computadores, link de dados, entre outros;
- Central de Serviços: *software* destinado ao atendimento de demandas internas da BHIP e que possui alguns serviços com interface externa;
- Dados: são qualquer informação que possui valor para uma organização ou indivíduo. Esse valor pode ser tanto tangível (como dados financeiros ou informações de clientes) quanto intangível (como propriedade intelectual ou conhecimento).
- Dispositivo: aparelho ligado ou adaptado a instrumento ou máquina, que se destina a alguma função adicional ou especial;
- Evento: ação com potencial para causar um dano, porém o dano ainda não ocorreu ou não foi identificado;
- *Hardware*: o hardware, circuitaria, material ou ferramental é a parte física do computador, ou seja, é o conjunto de componentes eletrônicos, circuitos integrados e placas, que se comunicam através de barramentos;
- Incidente de Segurança da Informação: ação praticada que causa danos a segurança do meio corporativo;
- *Know-how*: conhecimento específico;
- *Malware*: código malicioso, programa malicioso, *software* nocivo/malicioso, é um programa de computador destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar danos, alterações ou roubo de informações. Alguns o conhecem por vírus, que é somente uma das categorias de *malware*;
- PSI: Política de Segurança da Informação;
- Recursos de segurança: controles de acesso lógico, físico e qualquer outro que garanta a segurança da informação, seguindo as premissas de integridade, confidencialidade e disponibilidade da informação;

- Recursos de Tecnologia da Informação: equipamentos eletroeletrônicos, sistemas e aplicativos que manipulam direta ou indiretamente informações, inclusive a própria informação;
- Senha: código secreto (*password*, palavra secreta) que autentica a identidade de uma chave de acesso;
- Servidores: Equipamentos configurados para gerenciar diversos serviços como: *e-mail*, rede, *firewall*, controlador de domínio;
- Sistemas: funções interligadas que automatizam um processo;
- Sistemas restritos: sistemas que somente pessoas autorizadas têm acesso através de senha ou permissões;
- Termo de Confidencialidade: Contrato legal que estabelece uma obrigação entre duas ou mais com objetivo de manter determinadas informações em sigilo.
- VPN: *Virtual Private Network* (Rede Privada Virtual) e descreve a oportunidade de estabelecer uma conexão de rede protegida ao usar redes públicas;
- Usuário: toda pessoa (física ou jurídica) expressamente autorizada pela BHIP a fazer acesso e uso aos seus procedimentos, sistemas, redes e/ou equipamentos, tais como colaboradores, visitantes, clientes, fornecedores, prestadores de serviços e demais partes interessadas pertinentes.

5 Recursos, Equipamentos, *Softwares*

A Política de Segurança da Informação para Terceiros é disponibilizada por meio do website eletrônico exclusivo da BHIP que pode ser acessado por meio do *link*:

https://www.bhip.com.br/politica-de-seguranca-da-informacao-para-terceiros/

6 Diretrizes

6.1 Uso da Informação

Os terceiros devem tratar com total confidencialidade todas as informações corporativas e dados pessoais recebidos da BHIP durante a prestação de serviços, utilizando-os exclusivamente para a execução das atividades contratadas.

Cada terceiro terá acesso apenas às informações, dados e recursos estritamente necessários para realizar seu trabalho.

Comprometem-se a manter sigilo e proteger a confidencialidade de todas as informações corporativas e dados pessoais da BHIP, incluindo inovações, segredos comerciais, marcas, criações e especificações técnicas e comerciais. É proibido divulgar, reproduzir, utilizar ou permitir o uso dessas informações por seus empregados ou terceiros para qualquer fim que não o relacionado à prestação do serviço.

Além disso, os terceiros não estão autorizados a divulgar informações ou fazer declarações sobre assuntos internos da BHIP em qualquer mídia ou rede social.

6.2 Proteção das Informações

Todas as informações produzidas, individualmente ou em conjunto, pelos terceiros a serviço da BHIP, sejam originadas ou derivadas de suas atividades, são de propriedade da organização, incluindo qualquer informação fornecida ou licenciada pela empresa.

Os terceiros devem zelar e proteger as informações não públicas da BHIP às quais tenham acesso, sendo proibida sua divulgação sem autorização prévia. Não é permitido copiar, compartilhar ou utilizar essas informações para fins pessoais ou de terceiros.

Além disso, os terceiros devem adotar medidas de segurança, técnicas e administrativas para proteger as informações e dados da BHIP, utilizando mecanismos como criptografia, controle de acesso, política de senhas e mascaramento de dados, entre outros aplicáveis.

6.3 Proteção de Dados Pessoais

Os terceiros devem conhecer e cumprir a Lei nº 13.709/2018 Lei Geral de Proteção de Dados (LGPD) e demais legislações relacionadas à proteção de dados pessoais e à privacidade de seus titulares. Devem garantir os meios necessários para a aplicação efetiva da lei e para assegurar o exercício dos direitos dos titulares dos dados.

Além disso, devem adotar medidas de segurança, técnicas e administrativas para proteger os dados pessoais sob sua responsabilidade contra acessos não autorizados, bem

como contra destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, seja acidental ou intencional.

6.4 Restrição de Acesso à Informação

O acesso às informações corporativas, dados pessoais e às funções de sistemas e aplicações é restrito e segue as diretrizes internas da BHIP. Para garantir a segurança, os seguintes controles são implementados:

- Gerenciamento de acessos por meio de menus específicos para funções de sistemas e aplicações;
- Aplicação da hierarquia de acessos;
- Controle sobre os dados acessíveis por terceiros;
- Definição de permissões para leitura, exclusão, escrita e execução;
- Restrição de acessos a outras aplicações, conforme a necessidade;
- Limitação das informações disponíveis nas saídas dos sistemas;
- Restrição de impressões e manuseios de vias físicas de documentos;
- Controles de segurança lógica e física, especialmente para a proteção de dados pessoais e sensíveis.

6.5 Acesso Físico

A área administrativa da BHIP é responsável por estabelecer as barreiras físicas necessárias para controlar o acesso e proteger as informações corporativas e dados pessoais da empresa.

Os usuários que eventualmente visitarem a sede da BHIP deverão respeitar as diretrizes de identificação de entrada, serem acompanhadas por colaborador autorizado e observar os ambientes que possuem acesso restrito.

A BHIP é monitorada em tempo real e 24h por dia x 7 dias por semana, por câmeras de vigilância posicionadas estrategicamente.

6.6 Locais Sensíveis

Os usuários devem respeitar as áreas designadas como de conteúdo sensível, cumprindo todas as regras e restrições, incluindo a proibição de registros fotográficos, gravações de áudio e vídeo, além da vedação ao compartilhamento de qualquer informação em mídias ou redes sociais.

6.7 Armazenamento de Informações

Os usuários devem informar à BHIP, quando solicitado, as medidas de segurança adotadas para a transmissão e armazenamento de informações corporativas e dados pessoais, garantindo a segregação de dados e controle de acesso (lógico e físico).

Devem manter rotinas de backup com cópias dos dados de produção, incluindo backup local e off-site, seguindo as melhores práticas de segurança da informação. As cópias devem ser armazenadas em locais seguros e testadas regularmente para garantir sua rastreabilidade, recuperação e confiabilidade em casos de emergência.

Documentos físicos devem ser arquivados de forma segura, com barreiras físicas a exemplo de trancas e biometria, e retidos conforme os prazos legais.

6.8 Descarte de Informação

Após o término da prestação de serviço, todas as informações corporativas e dados pessoais utilizados devem ter destinação final apropriada, quer sejam estes devolvidos à BHIP em até 30 (trinta) dias, e sempre que possível, acompanhados de um comprovante assinado pelo representante legal atestando a devolução, ou mediante envio de comprovação por parte do usuário sobre a destinação final dada. Esta ação possibilita que a BHIP possua controle sobre as informações partilhadas externamente.

6.9 Uso dos Recursos de Tecnologia

O uso dos recursos de tecnologia fornecidos pela BHIP deve seguir diretrizes de segurança e conformidade.

É proibido ao usuário acessar, propagar ou utilizar sites, aplicativos e conteúdos que:

- Violam leis ou regulamentos vigentes em qualquer nível (local, estadual, nacional ou internacional);
- Comprometem a privacidade, honra ou imagem de qualquer pessoa física ou jurídico, incluindo direitos autorais e propriedade intelectual;
- Promovam discriminação, assédio, ameaças ou perseguições, seja por raça, gênero, religião, etnia, nacionalidade ou condição social;
- Contêm material ofensivo, pornográfico, violento ou ilícito, incentivando condutas imorais ou criminosas;
- Façam apologia a crimes ou práticas prejudiciais à saúde física ou mental;
- Violam segredos empresariais ou estimulam pirataria sem a devida autorização legal;
- Distribuem spam, propagandas enganosas ou correspondências comerciais não autorizadas;
- Tentam acessar indevidamente sistemas da BHIP ou de terceiros (hacking);
- Introduzem vírus, malware ou qualquer outro elemento prejudicial ao ambiente tecnológico da BHIP.

Além disso, é proibido realizar atividades não contratadas ou agir de forma negligente, causando danos à rede, sistemas, equipamentos ou comprometendo a integridade das informações corporativas e dados pessoais.

6.10 Fornecimento de Recursos ou Dispositivos Corporativos

A BHIP fornecerá recursos ou dispositivos corporativos, como acesso a sistemas, rede, e-mail e VPN apenas quando necessário para garantir um acesso seguro às informações e ao ambiente interno de tecnologia.

O usuário deve seguir todas as políticas, normas e manuais disponibilizados, além de proteger fisicamente e garantir a integridade dos dispositivos cedidos, preservando as informações corporativas e dados pessoais da BHIP.

6.11 Uso de Dispositivos Móveis

A BHIP poderá autorizar, mediante solicitação, o uso de dispositivos móveis de terceiros para a execução dos serviços contratados. No entanto, a compatibilidade e configuração desses dispositivos são de responsabilidade do próprio terceiro.

A BHIP não fornece aplicativos, atualizações de sistema ou suporte tecnológico para dispositivos de terceiros, apenas oferece orientações quando necessário. Em alguns casos, poderá recomendar ou fornecer aplicativos específicos para garantir o acesso seguro às informações corporativas e dados pessoais.

Os usuários de dispositivos móveis de terceiros devem manter sistemas e aplicativos sempre atualizados, conforme as recomendações dos fabricantes, para reduzir falhas de segurança e vulnerabilidades. A responsabilidade pelas atualizações é inteiramente do terceiro.

6.12 Controle de Acesso

Os dispositivos móveis de usuários usados nas instalações da BHIP devem ser protegidos por senha ou outro controle de segurança para impedir acessos não autorizados. O usuário será responsável por proteger seus dispositivos que contenham informações corporativas e dados pessoais.

O acesso à rede interna da BHIP será avaliado e concedido conforme a necessidade, seguindo a Política de Segurança da Informação.

Usuário e senha fornecidos ao usuário são pessoais e intransferíveis, não podendo ser compartilhados. O usuário deve seguir todas as políticas, normas e procedimentos disponibilizados da BHIP, sendo responsável pelo uso seguro de suas credenciais.

A empresa terceirizada deverá informar imediatamente qualquer desligamento de funcionários para que seus acessos sejam cancelados no ambiente da BHIP.

6.13 Senhas de Acesso

Senhas seguras devem ser criadas para acessar dispositivos utilizados na prestação de serviços à BHIP, seja em equipamentos próprios ou corporativos. Recomenda-se seguir as melhores práticas:

- Criar senhas fortes, com pelo menos 8 caracteres, incluindo letras maiúsculas e minúsculas, números e caracteres especiais;
- Nunca compartilhar senhas, seja verbalmente, por escrito ou eletronicamente;
- Ativar a autenticação multifator (MFA) sempre que disponível;
- Alterar senhas imediatamente se houver suspeita de comprometimento ou tentativa de invasão;
- Alterar senhas periodicamente;
- Adotar senhas diferenciadas para as diferentes aplicações.

6.14 Proteção Contra Ameaças Cibernéticas

A BHIP adota medidas de proteção contra ameaças cibernéticas nas esferas aplicáveis. Uma vez na BHIP, usuários externos estão sujeitos ao monitoramento do firewall e bloqueios de categorias de acesso e conteúdos, enquanto medidas preventivas.

6.15 Uso de Software

O uso de software não licenciado ou pirata é ilegal e expressamente proibido, sendo considerado uma infração grave desta Política. Isso pode levar à rescisão do contrato e à aplicação de penalidades.

Se for identificado o uso indevido de software ou aplicativos, a BHIP poderá bloquear seu uso e adotar as medidas necessárias para evitar danos. Além disso, o terceiro será responsável por ressarcir qualquer prejuízo causado à BHIP.

6.16 Rede Cabeada, Wifi e Internet

Os terceiros deverão aceitar e seguir todas as políticas, normas e procedimentos da BHIP que lhe forem informados para a utilização da rede cabeada, *wifi* e internet.

6.17 Controles de Segurança no Ambiente de Terceiro

O terceiro que tratar (considerando e não se limitando a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação,

modificação, comunicação, transferência, difusão ou extração) as informações da BHIP em seu ambiente, deve seguir as seguintes diretrizes de segurança da informação:

6.18 Controles de Acesso

Manter um processo documentado de gerenciamento de acessos, garantindo que o acesso a dados e informações seja controlado e concedido apenas conforme necessário para a execução dos serviços. Deve-se preservar a confidencialidade, integridade, disponibilidade e a capacidade de recuperação dessas informações.

6.19 Trabalho Remoto

Na hipótese de trabalho remoto, o usuário deve atuar com máxima diligência para evitar o acesso não autorizado às informações da BHIP e adotar medidas de segurança avançadas.

O acesso remoto a sistemas e informações da BHIP exige autenticação do usuário, podendo incluir múltiplos fatores de autenticação, conforme a criticidade do sistema.

O trabalho remoto não deve ser realizado em locais sem privacidade (ex.: aeroportos, salas de reunião, transportes públicos). Recomenda-se o uso de dispositivo pessoal com conexão 4G ou 5G para maior segurança.

Os acessos realizados no trabalho remoto na rede da BHIP são registrados e podem ser auditados a qualquer momento. A BHIP pode bloquear acessos caso identifique irregularidades.

6.20 Desenvolvimento Seguro de Sistemas

Os sistemas devem ser desenvolvidos seguindo padrões de segurança reconhecidos. Os usuários devem consultar as boas práticas de desenvolvimento seguro contidos no Anexo I desta PSI.

6.21 Monitoramento dos Serviços

Garantir o monitoramento contínuo dos serviços, a conformidade com a legislação vigente e a adesão às certificações exigidas pela BHIP.

6.22 Revogação de Acesso

Todo e qualquer tipo de acesso disponibilizado aos usuários será revogado ao término do contrato e/ou ao encerramento da relação empresarial e/ou em caso de substituição do usuário, violação de políticas ou por determinação da BHIP a qualquer tempo, sem aviso prévio.

6.23 Mesa Limpa e Tela Limpa

Para proteger informações da BHIP, o usuário deve garantir que dados sigilosos não fiquem expostos. Recomenda-se:

- Não deixar documentos impressos em locais visíveis ou de uso comum;
- Bloquear telas de computadores e dispositivos ao se ausentar;
- Remover documentos de impressoras e copiadoras imediatamente após o uso.

6.24 Gestão de Vulnerabilidade

Recomenda-se implementar medidas para prevenir, detectar e reduzir vulnerabilidades cibernéticas, incluindo autenticação segura, criptografia, detecção de intrusões, testes periódicos e segmentação de redes.

6.25 Gestão de Incidente

Recomenda-se manter um processo estruturado de resposta a incidentes e fornecer, quando solicitado, um relatório de incidentes ocorridos nos últimos 12 meses, classificando sua gravidade. A BHIP deve ser informada sobre qualquer limitação que possa afetar a prestação de serviços ou a conformidade regulatória.

Recomenda-se disponibilizar um canal de comunicação para relatos de incidentes e/ou eventos suspeitos.

6.26 Continuidade do Negócio

Recomenda-se ter um plano de continuidade do negócio para garantir que incidentes e/ou situações de emergência não prejudiquem os serviços prestados à BHIP.

6.27 Certificações e Auditorias Independentes

Fornecer à BHIP, quando solicitado, certificações necessárias e relatórios de auditorias independentes relacionadas aos controles adotados.

6.28 Auditoria e Conformidade

A BHIP pode, mediante aviso prévio, proceder com fiscalizações e/ou auditorias em seus equipamentos, procedimentos e processos cedidos e/ou compartilhados com os usuários terceiros para garantir o cumprimento das diretrizes desta Política de Segurança da Informação e atendimento a requisitos legais e normativos aplicáveis.

6.29 Treinamento e Conscientização

Os terceiros devem oferecer treinamento periódico em segurança da informação para todos os seus usuários correlacionados que tenham acesso às informações da BHIP.

A BHIP recomenda que todos os usuários busquem meios de conscientização e conhecimento sobre a importância da segurança da informação no mundo corporativo e pessoal.

6.30 Incidentes e Contato

Em caso de necessidade de contato e/ou para relatos de incidentes que comprometam as diretrizes desta PSI, os usuários devem recorrer aos meios de comunicação informados no *website* da BHIP.

6.31 Vigência da PSI para Terceiros

As regras e diretrizes desta Política entram em vigor na data de implantação deste documento e abrangem todas as áreas, colaboradores e usuários de recursos e informações pertencentes à BHIP. A BHIP se resguarda ao direito de revisar sua PSI a qualquer tempo, sem prévio aviso, assegurando sua conformidade e atualização diante de requisitos legais, técnicos, normativos e outros aplicáveis.

7 Histórico das Revisões

Tabela 1 - Histórico das revisões

REVISÃO	DATA	NATUREZA DA ALTERAÇÃO
00	11/03/2025	Versão inicial.

8 Anexo I – PREMISSAS DA BHIP PARA DESENVOLVIMENTO SEGURO

Diante das inúmeras possibilidades que o mundo da tecnologia oferece, é cada vez mais difícil delinear os recursos, aproveitar de melhor maneira as inovações e se defender de incidentes e crimes cibernéticos.

A BHIP entende essa dificuldade e como uma das recomendações para tratar de se desenvolver softwares completamente livres de falhas de segurança, apresentamos a utilização de um conceito chamado Security By Design ou Segurança por Design para aumentar a segurança em todas as fases de criação, ou até mesmo de manutenção, de um sistema, minimizar e gerenciar riscos decorrentes de ataques que se sabe que podem ocorrer a qualquer momento.

A ideia é seguir alguns princípios pré-definidos durante todo o ciclo de vida do desenvolvimento, evitando invasões, violações de segurança cibernética ou danos aos dados de todo o desenvolvimento.

As diretrizes recomendadas são:

- **Princípio do Privilégio Mínimo**

Garantir que as pessoas tenham acesso apenas ao que for estritamente necessário para realizar o trabalho. O acesso a outras funcionalidades deve estar restrito como forma de minimizar riscos.

- **Princípio da Separação de Funções**

Garantir que as demandas não sejam muito grandes, separando em blocos de funções. Demandas grandes requerem muitas permissões de acesso.

- **Princípio da Defesa em Profundidade**

Trata-se de impedir o acesso forçado de terceiros ao sistema. Configurar sistemas que informarão quando a segurança designada falhar.

- **Princípio de Falhar com Segurança**

Necessário reconhecer que a falha vai aparecer cedo ou tarde. Um sistema projetado para falhar com segurança só concede acesso a partes do sistema quando todas as etapas do processo são concluídas com êxito.

- **Princípio do Design Aberto**

A segurança do sistema não deve depender do sigilo de sua implementação. Este é um princípio particularmente importante para conceitos de segurança como implementações criptográficas. Em linhas gerais, o princípio garante que o sistema esteja protegido, independentemente de alguém mal-intencionado obter acesso ao seu código.

- **Princípio de Evitar Segurança por Obscuridade**

Um melhor design para o sistema é aquele em que a conta com acesso total não existe. E se for necessário criá-la, é importante fazer gestão ativa, para evitar incidentes de segurança.

- **Princípio de Minimização da Área de Superfície de Ataque**

O importante aqui é restringir as funções que os usuários podem acessar, para reduzir potenciais vulnerabilidades. Muitas das partes de um software são como janelas. A princípio, podem parecer interessantes, mas trazem consigo a possibilidade de expor funcionalidades que levam a bugs. Assim, para minimizar a área de superfície de ataque é importante questionar se determinado recurso é mesmo necessário. Às vezes, ao redesenhar um recurso para torná-lo mais simples, a segurança geral do aplicativo melhora.

Como recomendações adjacentes deve-se atualizar e testar os sistemas regularmente. Os sistemas precisam ser atualizados com as versões mais recentes. O motivo é que as falhas de segurança precisam ser corrigidas o mais rápido possível. A segurança e a vulnerabilidade dos sistemas devem ser revisadas por meio de verificações contínuas de segurança.

As arquiteturas dos sistemas devem ser preferencialmente simples ao desenvolver controles de segurança. Sistemas complexos são difíceis de corrigir quando ocorrem erros e a solução dos problemas pode ser demorada, o que oferece uma oportunidade para os cibercriminosos explorarem, colocando o aplicativo em maior risco.

Prezar pelas boas-práticas de desenvolvimento e seguir os princípios Segurança por Design são certeza de um resultado excelente do sistema e para as parcerias que dele se utilizarem.